BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants:	**HAEGENDOREN, Ben Van, et al.**
Serial Number:	**10/561,142**
Atty. Dkt:	**PF030103**
Filing Date:	**December 19, 2005**
For:	**NETWORK EQUIPMENT AND A METHOD FOR MONITORING THE START UP OF SUCH AN EQUIPMENT**
Art Unit:	**2114**
Examiner:	**LOHN, Joshua A.**

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

In response to the final Office Action dated December 9, 2009, and further to the Notice of Appeal filed on March 9, 2010, Appellants hereby submit an Appeal Brief in accordance with 37 C.F.R. §41.37 for the above-referenced application.

I. Real Party in Interest

The real party in interest is Thomson Licensing LLC.

II. Related Appeals and Interferences

There are no prior or pending appeals, interferences, or judicial proceedings known to Appellants, the Appellants' legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. Status of Claims

Claims 1, 3-14 and 16-22 are pending in this application, and are rejected. Claims 2 and 15 are cancelled. The rejection of claims 1, 3-14 and 16-22 is being appealed.

IV. Status of Amendments

No amendment subsequent to the final rejection of December 9, 2009 has been filed.

V. Summary of Claimed Subject Matter

Independent claim 1 defines network equipment for providing a connection to a local network, said local network comprising at least one software server (see, for example, page 2, lines 1-2), said network equipment comprising:

a memory for storing software (see, for example, page 2, line 3);

means for providing a connection to said local network (see, for example, element 9 of FIG. 1 and page 2, line 5); and

means for monitoring a start up of the network equipment to detect a software start up failure (see, for example, element 10 of FIG. 1 and page 2, lines 6-7), and for generating a software start up failure signal in response to detecting said software start up failure, said software start up failure signal being broadcast on the local network for reception by said at least one software server (see, for example, page 2, lines 8-11), said software start up failure signal comprising information specifying at least one of:

(i) a nature of said software start up failure, an identification of replacement software to be downloaded, and an identification of a version of the software currently stored in the memory (see, for example, page 4, lines 24-31 and page 5, lines 4-8);

(ii) said nature of said software start up failure, and said identification of replacement software to be downloaded (see, for example, page 4, lines 24-31 and page 5, lines 4-8); and

(iii) said nature of said software start up failure, and said identification of said version of the software currently stored in the memory (see, for example, page 4, lines 24-31 and page 5, lines 4-8).

Dependent claim 10 further defines the network equipment according to claim 1, and states wherein the monitoring means (see, for example, element 10 of FIG. 1) comprises:

a timer to determine a time limit for a software start up (see, for example, page 9, lines 13-15);

means for launching the software start up (see, for example, element 10 of FIG. 1 and page 9, lines 13-15); and

means for generating said software start up failure signal if the software start up is not completed before an end of the time limit (see, for example, element 10 of FIG. 1 and page 9, lines 17-19).

Dependent claim 12 further defines the network equipment according to claim 1, and states further comprising an alarm connected to the monitoring means for communicating the software start up failure to the user (see, for example, page 5, lines 12-13).

Independent claim 16 defines a method for monitoring a software start up for network equipment, the network equipment comprising a memory for storing software and a connector for providing a connection to a local network comprising at least one software server (see, for example, page 2, lines 24-27), said method comprising the steps of:

monitoring the software start up for the network equipment to detect a software start up failure (see, for example, page 2, lines 29-30);

generating a software start up failure signal in response to detecting said software start up failure (see, for example, page 2, lines 31-32); and

automatically broadcasting the software start up failure signal on the local network for reception by said at least one software server (see, for example, page 2, lines 33-34), wherein the software start up failure signal comprises information specifying at least one of:

(i) a nature of said software start up failure, an identification of replacement software to be downloaded, and an identification of a version of said software currently stored in said memory (see, for example, page 4, lines 24-31 and page 5, lines 4-8);

(ii) said nature of said software start up failure, and said identification of replacement software to be downloaded (see, for example, page 4, lines 24-31 and page 5, lines 4-8); and

(iii) said nature of said software start up failure, and said identification of said version of the software currently stored in said memory (see, for example, page 4, lines 24-31 and page 5, lines 4-8).

Independent claim 19 defines network equipment for providing a connection to a local network, said local network comprising at least one software server (see, for example, page 2, lines 1-2), said network equipment comprising:

a memory for storing software (see, for example, page 2, line 3);

means for providing a connection to said local network (see, for example, element 9 of FIG. 1 and page 2, line 5); and

means for monitoring a start up of the network equipment to detect a software start up failure (see, for example, element 10 of FIG. 1 and page 2, lines 6-7), and for generating a software start up failure signal in response to detecting said software start up failure, said software start up failure signal being broadcast on the local network for reception by said at least one software server (see, for example, page 2, lines 8-11), said software start up failure signal comprising information specifying a nature of said software start up failure (see, for example, page 4, lines 24-31 and page 5, lines 4-8).

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejection are presented for review in this appeal:

A. The rejection of claims 1, 3-9, 11, 13, 14 and 16-22 under 35 U.S.C. §103(a) based on the proposed combination of U.S. Patent No. 5,940,074 issued to Britt Jr. et al. (hereinafter, "Britt") and U.S. Patent No. 7,251,725 issued to Loison et al. (hereinafter, "Loison"); and

B. The rejection of claims 10 and 12 under 35 U.S.C. §103(a) based on the proposed combination of Britt, Loison and U.S. Patent Publication No. 2002/0095619 by Marsh (hereinafter, "Marsh").

VII. Argument

A. Patentability of Claims 1, 3-9, 11, 13, 14 and 16-22

The rejection of claims 1, 3-9, 11, 13, 14 and 16-22 under 35 U.S.C. §103(a) based on the proposed combination of Britt and Loison should be reversed for at least the following reasons.

It is first noted that independent claim 1 recites:

> "Network equipment for providing a connection to a local network, said local network comprising at least one software server, said network equipment comprising:
> a memory for storing software;
> means for providing a connection to said local network; and
> means for monitoring a start up of the network equipment to detect a software start up failure, and for generating a software start up failure signal in response to detecting said software start up failure, said software start up failure signal being broadcast on the local network for reception by said at least one software server, said software start up failure signal comprising information specifying at least one of:
> (i) a nature of said software start up failure, an identification of replacement software to be downloaded, and an identification of a version of the software currently stored in the memory;
> (ii) said nature of said software start up failure, and said identification of replacement software to be downloaded; and
> (iii) said nature of said software start up failure, and said identification of said version of the software currently stored in the memory." (emphasis added)

As indicated above, independent claim 1 defines network equipment comprising a memory for storing software, means for providing a connection to a local network, and means for monitoring a start up of the network equipment to detect a software start up failure. In response to detecting the software start up failure, the monitoring means generates a software start up failure signal which is broadcast on the local network for reception by at least one software server. The software start up failure signal comprises information specifying at least one of: (i) a nature of said software start up failure, an identification of replacement software to be downloaded, and an identification of a version of the software currently stored in the memory; (ii) said nature of said software start up failure, and said identification of replacement software to be downloaded; and (iii) said nature of said software start up failure, and said identification of said version of the software currently stored in the memory. Independent claims 16 and 19 recite subject matter similar to independent claim 1.

Neither Britt nor Loison, whether taken individually or in combination, discloses or suggests each and every element of independent claims 1, 16 or 19. On page 3 of the final Office Action dated December 9, 2009, the Examiner alleges that the "means ... for generating a software start up failure signal in response to detecting said software start up failure", as recited by independent claim 1, is disclosed in column 8, lines 14-32 of Britt, where the initiation of an error download routine in Britt allegedly corresponds to the claimed "software start up failure signal". This error download routine of Britt is performed at step 604 of FIG. 6, and is further described in column 9, lines 35-57 and FIG. 9 thereof.

According to Britt, the aforementioned error download routine starts with client system 1 connecting to server 5 (see FIG. 1) using a default toll-free number. Once connected, client system 1 obtains a local connection script from server 5 (see step 901 of FIG. 9). Here, Appellants note that the local connection script does not comprise any information specifying "a nature of said software start up failure" as recited by independent claims 1, 16 and 19.

Later on page 4 of the final Office Action dated December 9, 2009, the Examiner alleges that the "indication of which file, default or upgrade, to download is an identification of the nature of the startup failure" and is disclosed in column 9, lines 50-51 (i.e. step 904 of FIG. 9) of Britt. In response, Appellants note that the request made at step 904 of Britt does not correspond to the initiation of the error download routine, which is alleged by the Examiner to correspond to the claimed "software start up failure signal" (see above). That is, the request made at step 904 of Britt is sent after the error download routine has started (i.e., after the client system has been connected to the default server). Accordingly, the Examiner is inconsistent is his allegations of what constitutes the claimed "software start up failure signal".

Finally, in the description of step 904 of Britt, it is indicated that the request comprises an indication of the replacement software to be downloaded and the software version. However, this request does not include any information specifying "a nature of said software start up failure" as recited by independent claims 1, 16 and 19. Accordingly, Appellants respectfully submit that Britt does not disclose or suggest, *inter alia*, the claimed "software start up failure signal" that comprises information specifying "a nature of said software start up failure" as recited by independent claims 1, 16 and 19.

On page 4 of the final Office Action dated December 9, 2009, the Examiner admits that "Britt fails to disclose the network communication being on a local network with the start up failure signal being only sent on a local network" (emphasis added). To remedy this admitted deficiency of Britt, the Examiner relies on Loison, and specifically cites column 1, lines 17-20 and 31-38 thereof alleging that the DHCP DISCOVER signal referred to in column 1, lines 31-38 of Loison corresponds to the claimed "software start up failure signal". In response, Appellants note that the DHCP DISCOVER signal of Loison is a well-known DHCP message that is adapted to reach a DHCP server, and is not a "software start up failure signal" as claimed. On page 2 of the final Office Action dated December 9, 2009, the Examiner responds to this point by alleging that the DHCP in Loison is used to recover from boot failure (citing column 1, lines 16-22 thereof) and therefore is acting as a startup failure recovery signal for

Loison. In response, however, Appellants note that column 1, lines 16-22 of Loison deals with remote boot processes, and in particular, to downloading a boot image if a boot fails at a client machine. However, this cited passage does not indicate that DHCP is used to recover from boot failure. Accordingly, for at least the foregoing reasons, Appellants respectfully submit that Loison is unable to remedy the admitted deficiency of Britt.

Appellants further note that independent claims 1, 16 and 19 each states that the "software start up failure signal" is broadcast on the local network. This conforms to Appellants' description, where the "software start up failure signal" is included in a BOOTP request. Although BOOTP is not described in detail in the application itself, BOOTP is a well-known standard, and a BOOTP request is a broadcast message. Here, Appellants note that Britt does not disclose broadcasting a request signal between the client system and the server. Rather, in Britt, the requests are sent in a point-to-point manner between the client system and the server. On page 2 of the final Office Action dated December 9, 2009, the Examiner responds to these points by simply alleging that Loison clearly discloses the broadcast of a message when taken in combination with Britt. However, the Examiner doesn't provide any details regarding how Loison and Britt disclose the broadcast of a message. Moreover, and more specifically, the Examiner doesn't indicate how the cited prior art discloses the "software start up failure signal being broadcast on the local network", as claimed.

Therefore, for at least the foregoing reasons, Appellants submit that independent claims 1, 16 and 19 (and their respective dependent claims) are non-obvious over the proposed combination of Britt and Loison, and respectfully request that the Board reverse the rejection of claims 1, 3-9, 11, 13, 14 and 16-22.

B. Patentability of Claims 10 and 12

The rejection of claims 10 and 12 under 35 U.S.C. §103(a) based on the proposed combination of Britt Jr., Loison and Marsh should be reversed for at least the following reasons. Marsh is unable to remedy the deficiencies of the proposed combination of Britt and Loison pointed out above in connection with independent claim

1, from which claims 10 and 12 depend. Accordingly, claims 10 and 12 are deemed non-obvious over the proposed combination of Britt, Loison and Marsh, and Appellants respectfully request that the Board reverse the rejection of claims 10 and 12.

VIII. Claims Appendix

1. Network equipment for providing a connection to a local network, said local network comprising at least one software server, said network equipment comprising:

a memory for storing software;

means for providing a connection to said local network; and

means for monitoring a start up of the network equipment to detect a software start up failure, and for generating a software start up failure signal in response to detecting said software start up failure, said software start up failure signal being broadcast on the local network for reception by said at least one software server, said software start up failure signal comprising information specifying at least one of:

(i) a nature of said software start up failure, an identification of replacement software to be downloaded, and an identification of a version of the software currently stored in the memory;

(ii) said nature of said software start up failure, and said identification of replacement software to be downloaded; and

(iii) said nature of said software start up failure, and said identification of said version of the software currently stored in the memory.

3. The network equipment according to claim 1, wherein the software comprises at least one of:

a boot program;

configuration data; and

firmware.

4. The network equipment according to claim 3, wherein the software comprises said firmware, and the monitoring means comprises:

means for checking a current firmware verification pattern; and

means for generating said software start up failure signal when said current firmware verification pattern is not valid.

5. The network equipment according to claim 1, wherein the monitoring means comprises:

means for calculating a checksum of the software currently stored in said memory;

means for comparing said calculated checksum to a previously stored checksum; and

means for generating the software start up failure signal when said calculated checksum is not identical to the previously stored checksum.

6. The network equipment according to claim 3, wherein the monitoring means comprises:

means for checking for a presence of the firmware in the memory;

means for rebooting the network equipment if the firmware is not stored in the memory; and

means for generating said software start up failure signal if the firmware is not stored in the memory.

7. The network equipment according to claim 1, wherein the monitoring means comprises:

means for monitoring downloading of replacement software in the memory; and

means for rebooting the network equipment and for generating said software start up failure signal if a problem is detected during said downloading.

8. The network equipment according to claim 3, wherein the software comprises said firmware, and the network equipment comprises:

means for writing a replacement firmware verification pattern corresponding to replacement firmware downloaded in the memory if said replacement firmware is properly recorded in said memory.

9. The network equipment according to claim 1, wherein the monitoring means comprises:

means for monitoring a process of loading said software in said memory; and

means for rebooting the network equipment and for generating said software start up failure signal if a problem is detected during said loading.

10. The network equipment according to claim 1, wherein the monitoring means comprises:

a timer to determine a time limit for a software start up;

means for launching the software start up; and

means for generating said software start up failure signal if the software start up is not completed before an end of the time limit.

11. The network equipment according to claim 1, further comprising user activation means connected to the monitoring means for enabling a user to manually request a download of replacement software.

12. The network equipment according to claim 1, further comprising an alarm connected to the monitoring means for communicating the software start up failure to the user.

13. The network equipment according to claim 1, wherein the monitoring means comprises:

means for checking a setting of a failure flag; and

means for generating the software start up failure signal and for transmitting the software start up signal on the local network in response to detecting that the failure flag is set.

14. The network equipment according to claim 1, wherein an indication of the nature of the software start up failure comprises a series of status flags.

16. A method for monitoring a software start up for network equipment, the network equipment comprising a memory for storing software and a connector for providing a connection to a local network comprising at least one software server, said method comprising the steps of:

monitoring the software start up for the network equipment to detect a software start up failure;

generating a software start up failure signal in response to detecting said software start up failure; and

automatically broadcasting the software start up failure signal on the local network for reception by said at least one software server, wherein the software start up failure signal comprises information specifying at least one of:

(i) a nature of said software start up failure, an identification of replacement software to be downloaded, and an identification of a version of said software currently stored in said memory;

(ii) said nature of said software start up failure, and said identification of replacement software to be downloaded; and

(iii) said nature of said software start up failure, and said identification of said version of the software currently stored in said memory.

17. The method according to claim 16, wherein the software start up failure signal comprises a request to the at least one software server for the download of the replacement software in the memory.

18. The method according to claim 16, wherein the software start up failure signal comprises an identification of the software start up failure for analysis by the at least one software server.

19. Network equipment for providing a connection to a local network, said local network comprising at least one software server, said network equipment comprising:

a memory for storing software;

means for providing a connection to said local network; and

means for monitoring a start up of the network equipment to detect a software start up failure, and for generating a software start up failure signal in response to detecting said software start up failure, said software start up failure signal being broadcast on the local network for reception by said at least one software server, said software start up failure signal comprising information specifying a nature of said software start up failure.

20. The network equipment according to claim 19, wherein the software comprises at least one of:

a boot program;

configuration data; and

firmware.

21. The network equipment according to claim 20, wherein the software comprises said firmware, and the monitoring means comprises:

means for checking a current firmware verification pattern; and

means for generating said software start up failure signal when said current firmware verification pattern is not valid.

22. The network equipment according to claim 19, wherein the monitoring means comprises:

means for calculating a checksum of the software currently stored in said memory;

means for comparing said calculated checksum to a previously stored checksum; and

means for generating the software start up failure signal when said calculated checksum is not identical to the previously stored checksum.

IX. Evidence Appendix

None.

X. Related Proceedings Appendix

None.

Please charge the fee for this Appeal Brief to Deposit Account 07-0832.

Respectfully submitted,

/Reitseng Lin/

By: Reitseng Lin
Reg. No. 42,804
Phone (609) 734-6813

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, New Jersey 08540
April 26, 2010